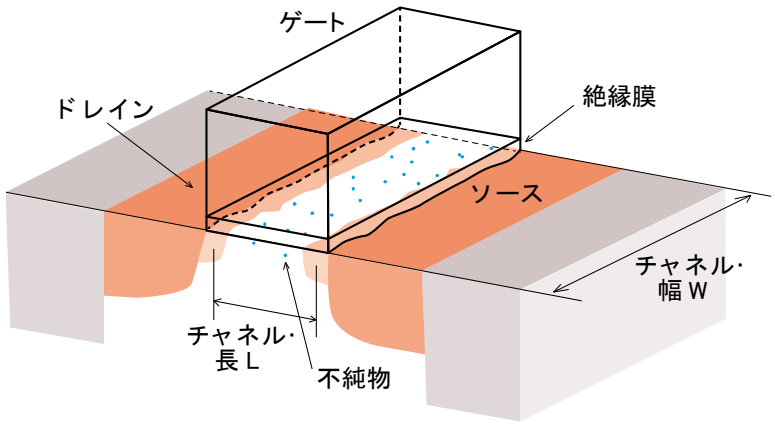
固有値を共有する
物理複製困難関数回路

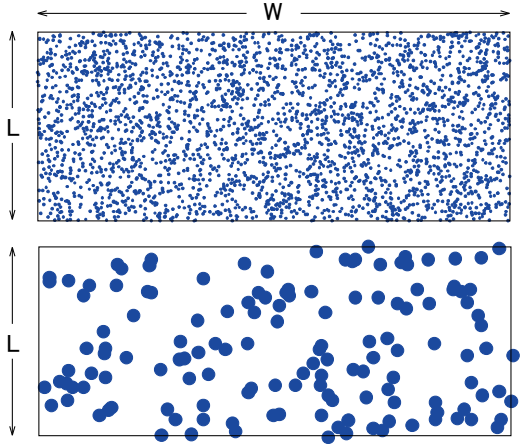
京都大学　大学院情報学研究科
通信情報システム専攻
教授 佐藤 高史

2019年5月16日

PUFとは

- Physical Unclonable Function
  物理複製困難関数
  - 入力に対し、ICチップに固有の応答を出力
    - チップの指紋のようなもの
  - 物理的ばらつきを利用
    - 製造の際に避けがたく生じるゆらぎ
      例) しきい値ばらつき、遅延時間ばらつき





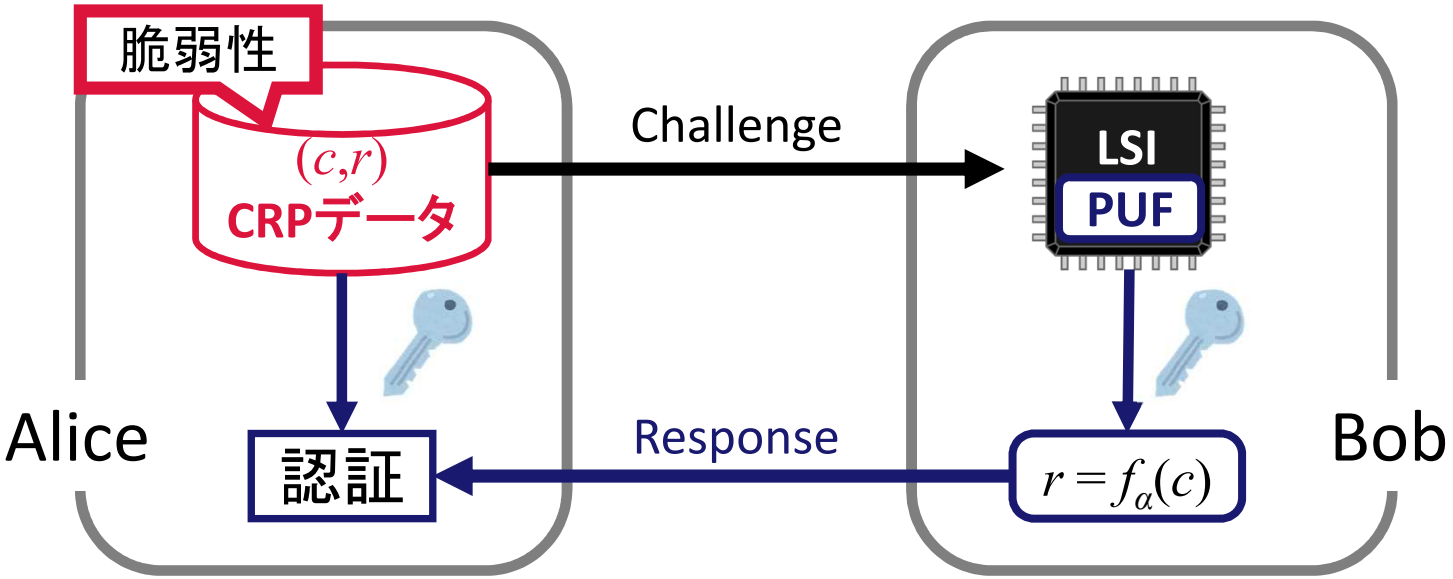
PUFの例とその性質

- SRAM PUF
  - メモリセルの初期状態を利用
- Arbiter PUF
  - 論理ゲートの遅延時間差を利用

- 重要な性質
  - 複製困難性 = unclonable
  - 予測困難性
  - 再現性など

従来PUFの使用手法(例:認証)

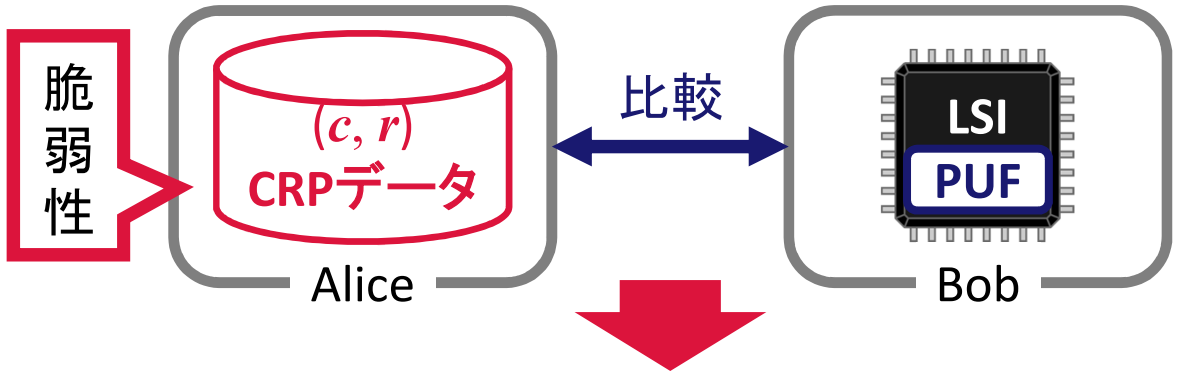
- 作成したCRPデータとチップのResponseを比較
  - CRP (c, r) : Challenge response pairs
  - 指数的に広いスペース
- 鍵が物理的ばらつきとして保存されるため高い安全性



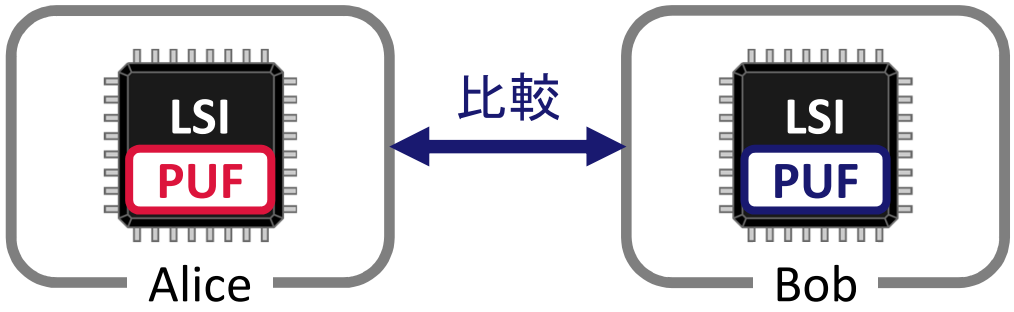
CRPデータが脆弱性となり得る

従来技術の課題と目的

- PUFの認証におけるCRPデータの脆弱性
  - あらかじめ十分な数のCRPを取得する必要がある



- データの事前取得や保存を不要とする
  - PUFのみによる認証を実現



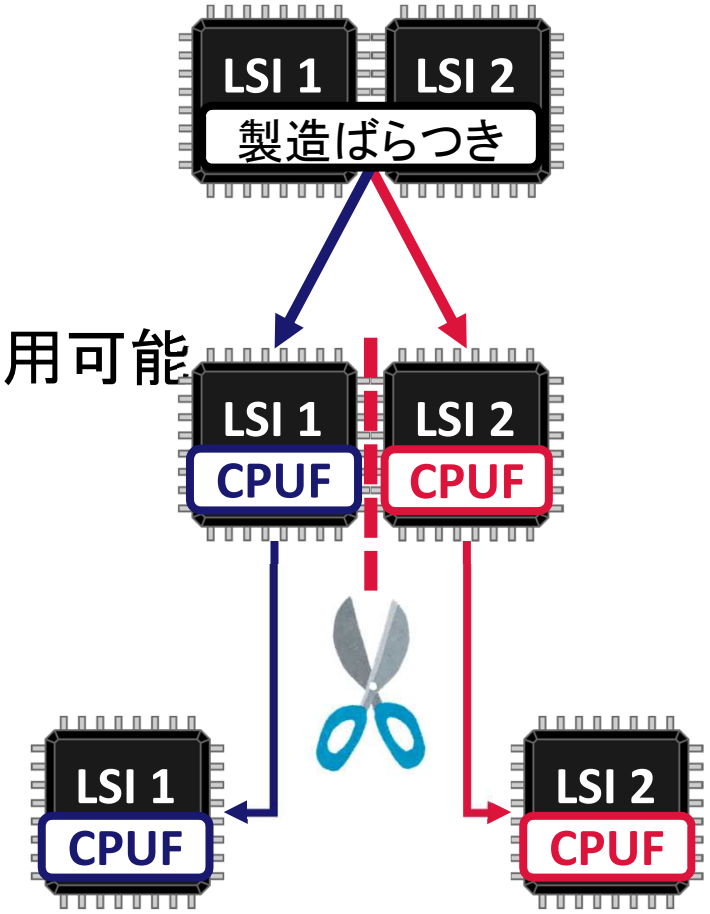
課題解決のアプローチ

- 固有値を共有するPUF(CPUF)を作成

- PUFは定義上複製不可能であるが、
  - 製造時に1回だけ複製を作る
  - 複製されたCPUFは、同じ入力に対し同じ応答
  - 各CPUFは、通常のPUFと区別がつかない
    - 複製困難性、予測困難性、再現性などPUFとしての性質を満たす

固有値を共有するPUF

- 「等価」な応答を返すPUF
  - 等価：同じ，反転 など
  - 複製：製造時のみ
  - 製造時：CPUFを複数生成
  - 製造後：複製困難，PUFとして使用可能

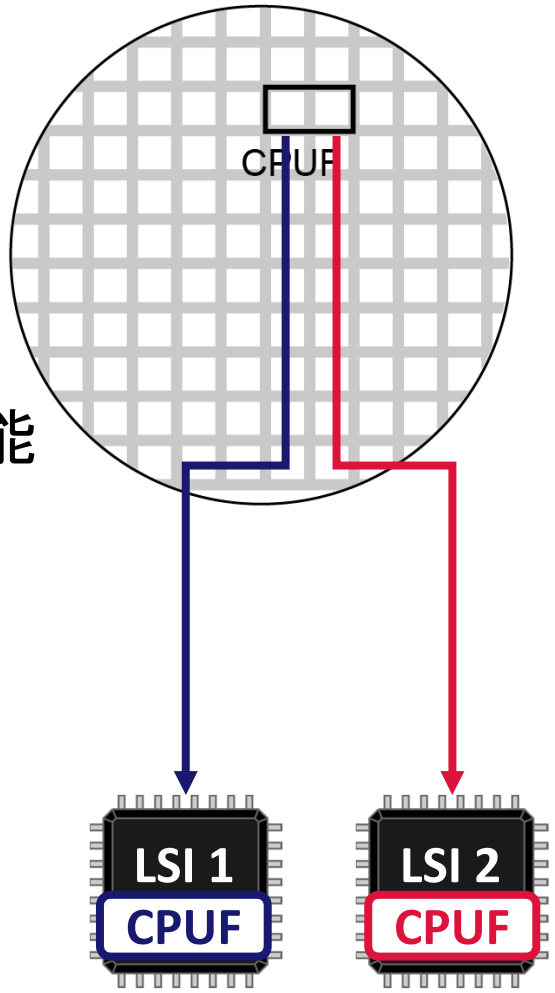


- 製造方法
  1. 複数のLSIを接続して製造
  2. 製造ばらつきからCPUFを作成
  3. 個々のCPUFをもつLSIに切断

CPUF同士で認証が可能（認証局やDBとの通信不要）

固有値を共有するPUF

- 「等価」な応答を返すPUF
  - 等価：同じ，反転 など
  - 複製：製造時のみ
  - 製造時：CPUFを複数生成
  - 製造後：複製困難，PUFとして使用可能

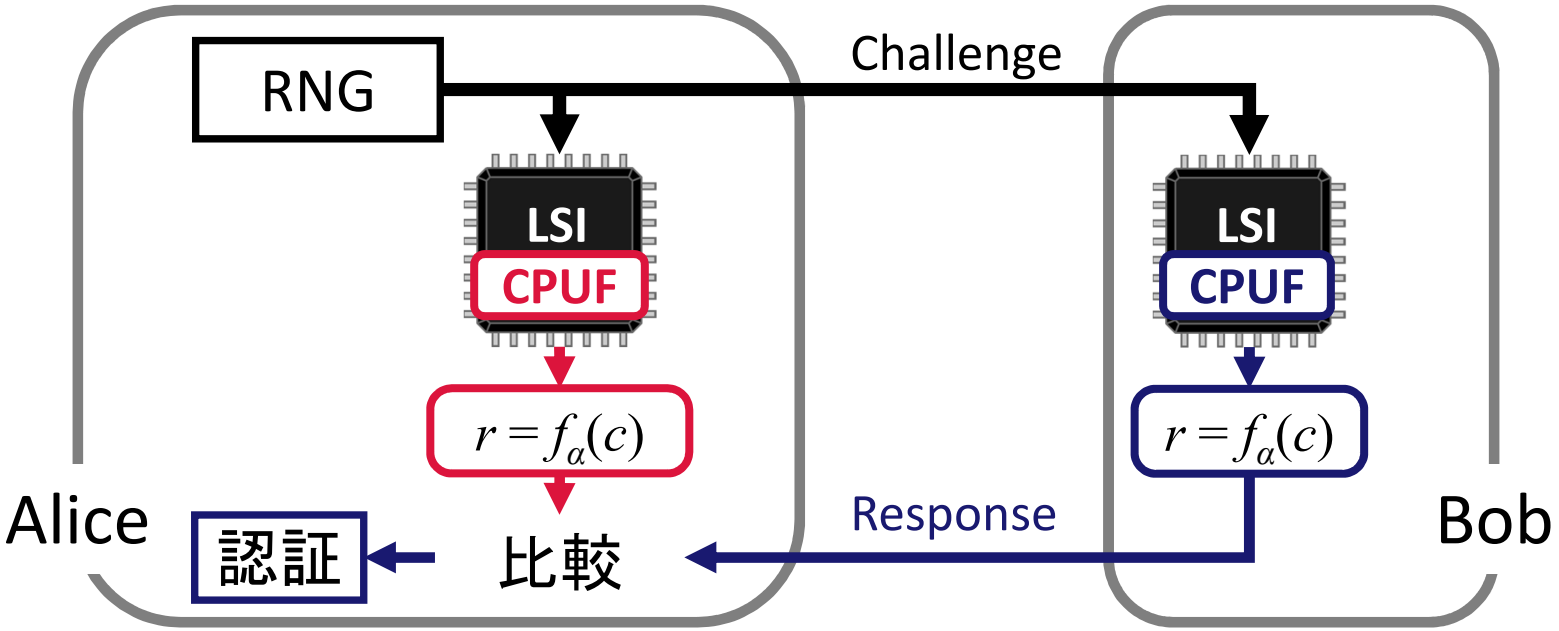


- 製造方法
  1. 複数のLSIを接続して製造
  2. 製造ばらつきからCPUFを作成
  3. 個々のCPUFをもつLSIに切断

CPUF同士で認証が可能（認証局やDBとの通信不要）

想定される用途 (1)

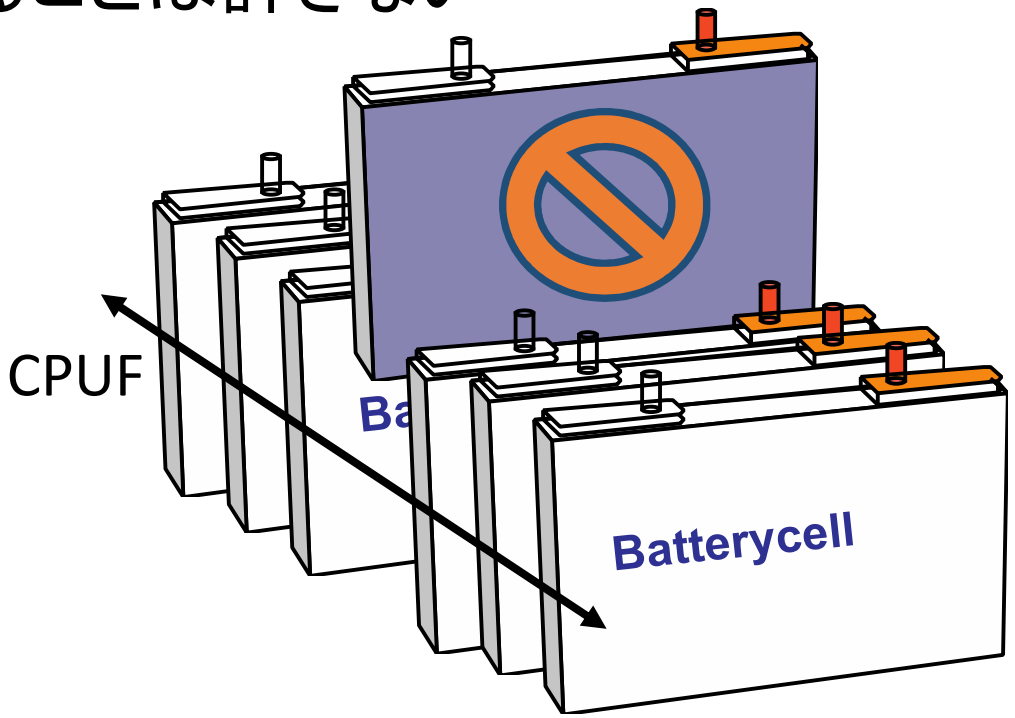
- 準備：AliceとBobがCPUFと乱数生成器（RNG）を持つ
  - RNG：チャレンジを生成
- 認証：Aliceの r とBobの r が等価であるか比較



安全性の高い認証を実現

想定される用途 (2)

- セットでの性能保証・再利用の防止
  - 同じ製品であっても異なるセットから得た部品を組み合わせることは許さない
- 組合せで使う対象を限定



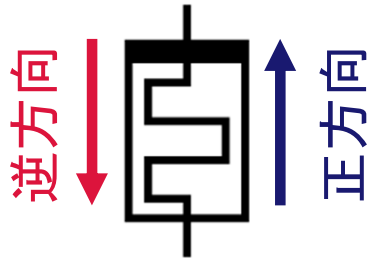
データベースとの通信を介さずに真正性を保証

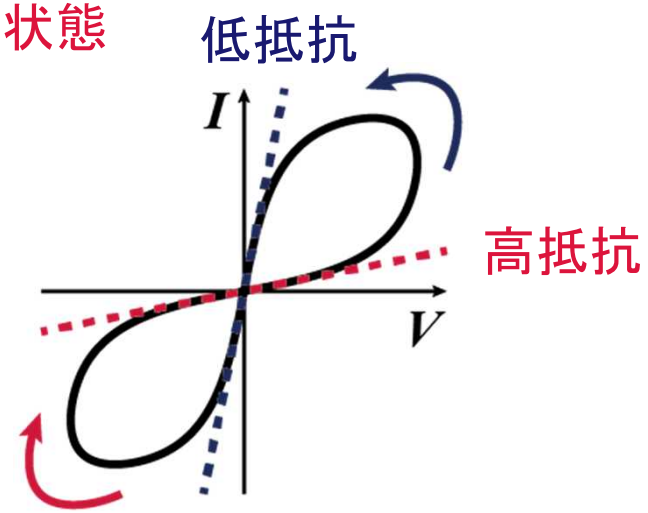
CPUFの作成方法

- 極言すると…
- ランダムな値が書いてあるセキュアメモリを作る
  - ただし、特定の個体間でランダムな値が一致することを保証する
  - 少部数ずつの乱数表を半導体技術で作ることに似ている
  - 外部から見えない形で応答を記憶
- 今回はRRAMを用いる2つの作り方を例示する

抵抗値変化型メモリ (RRAM)

- 第4の受動素子
  - 通過した電荷を抵抗値として記録可能
- 構造：二種類の金属で酸化金属を挟み込む
  - 物理的には導電性フィラメントの形成として説明される
    - 正方向にパルス電圧 → 低抵抗状態
    - 逆方向にパルス電圧 → 高抵抗状態

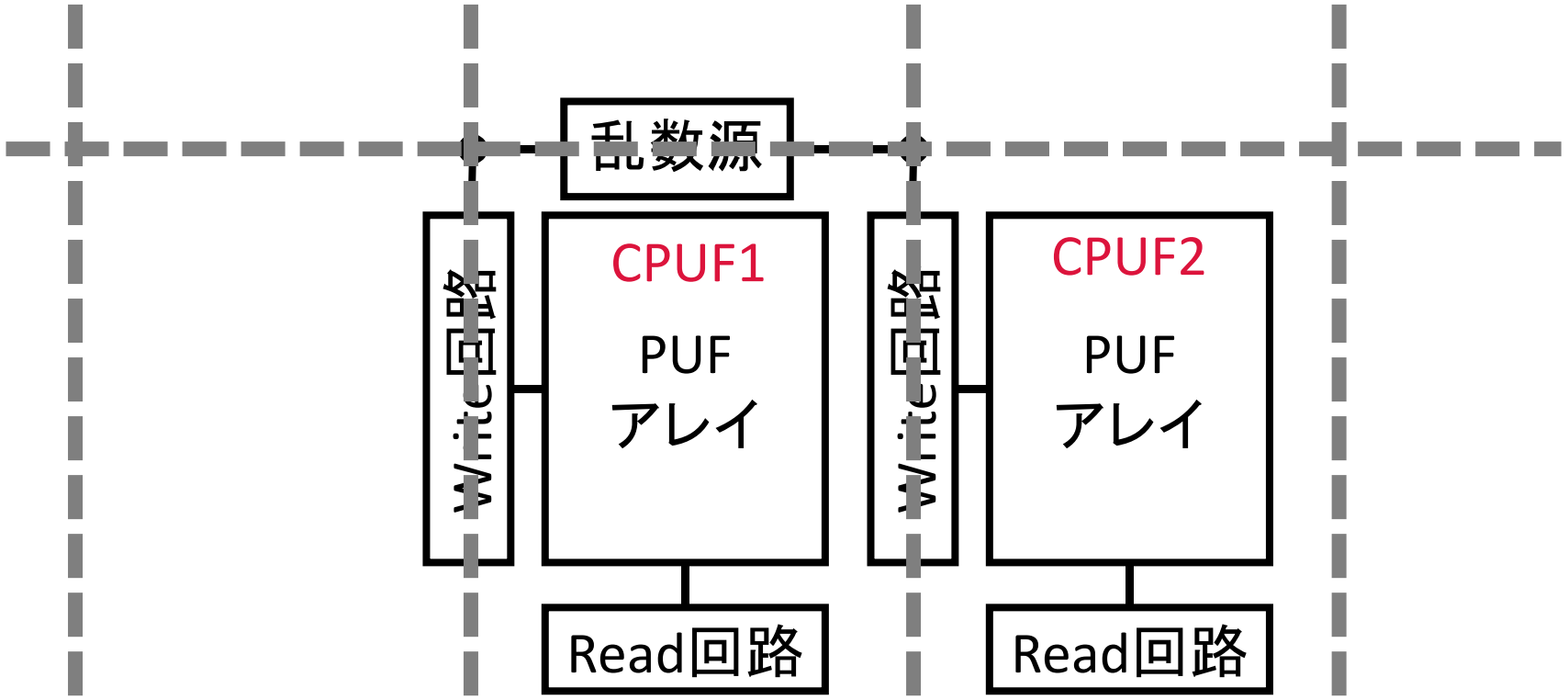




高抵抗状態と低抵抗状態をPUFの値として利用

CPUFの作成方法 (1)

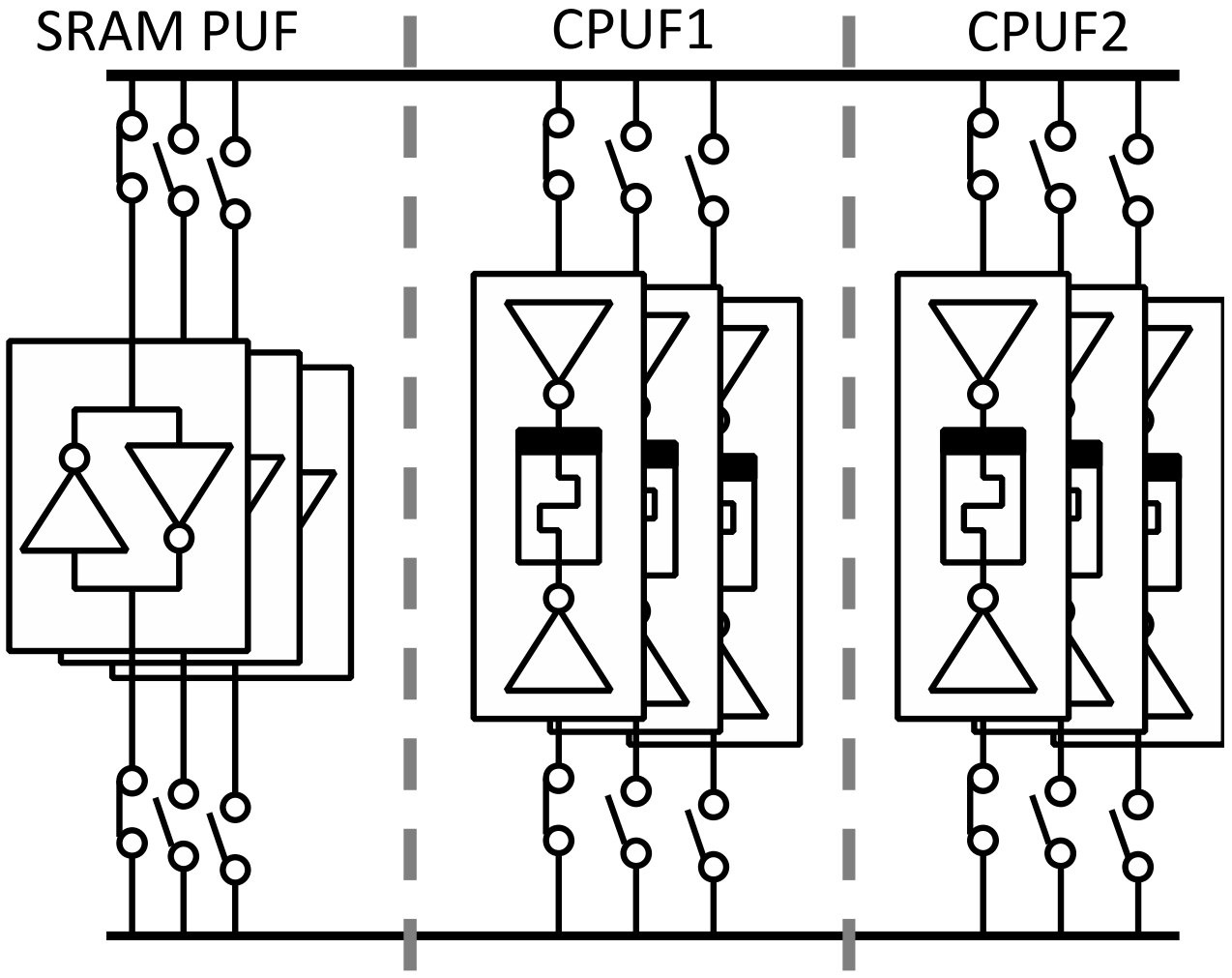
- 外部（or どれか一つのPUF）から値をコピー



ダイシング時に書き込みが不可能となる

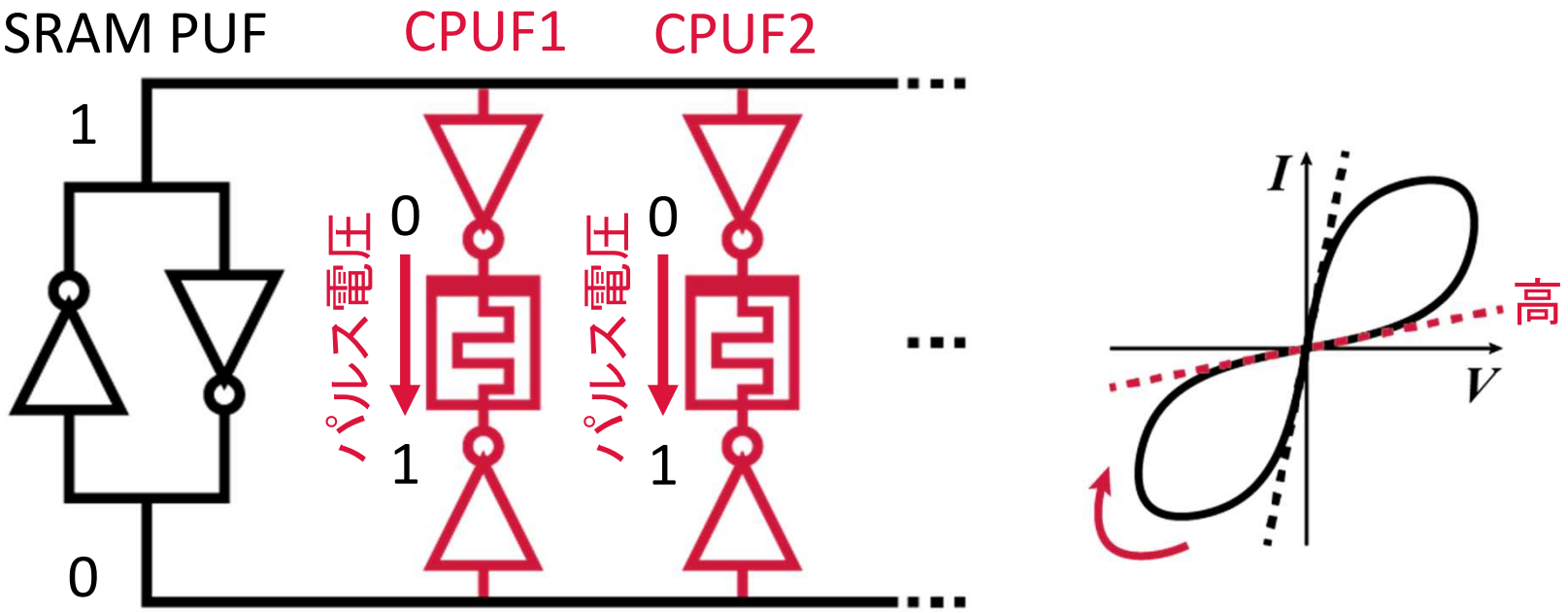
Shorted-INV CPUF : 基本回路

- SRAM PUFの値をRRAMに書き込む



Shorted-INV CPUF：基本回路

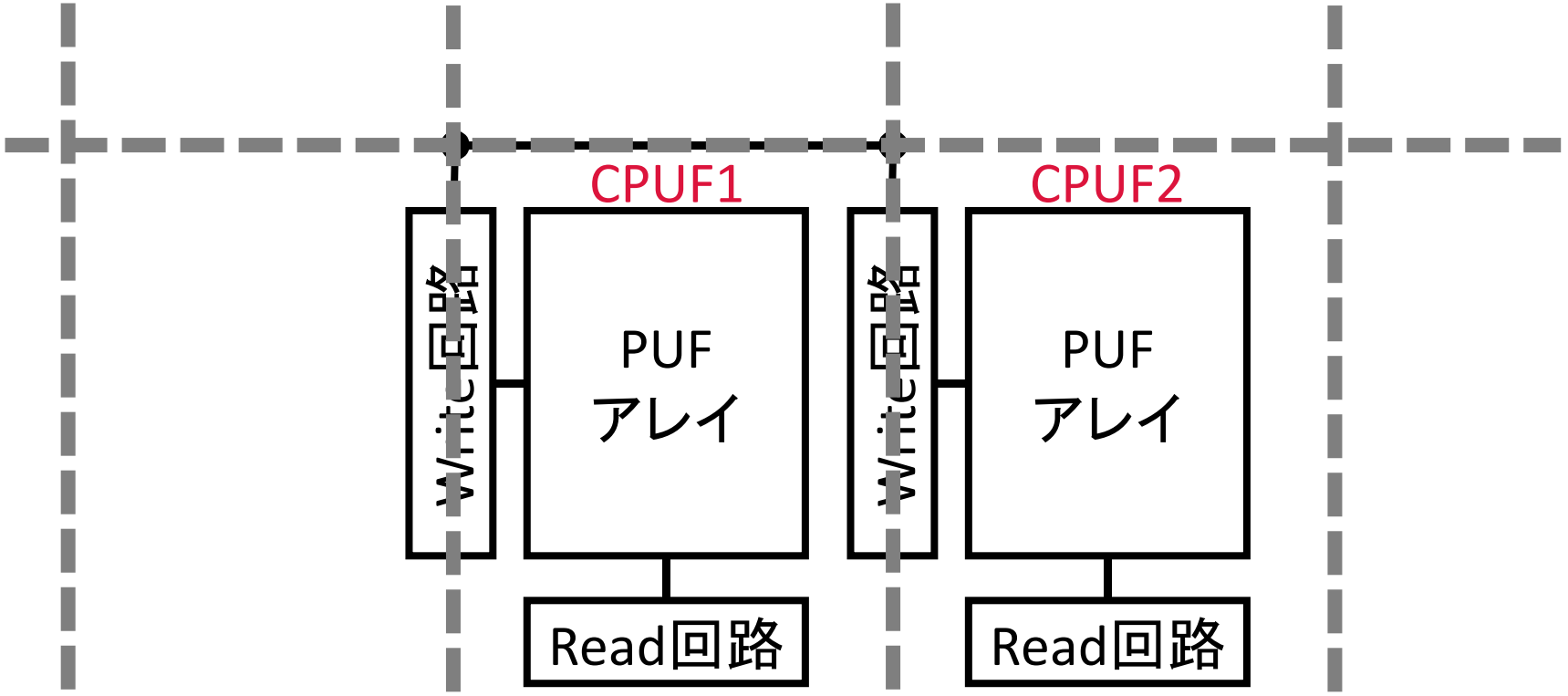
- SRAM PUFの値をRRAMに書き込み
  - SRAM PUF (0, 1)：RRAM高抵抗
  - SRAM PUF (1, 0)：RRAM低抵抗



接続されたRRAMがすべて同状態となる

CPUFの作成方法 (2)

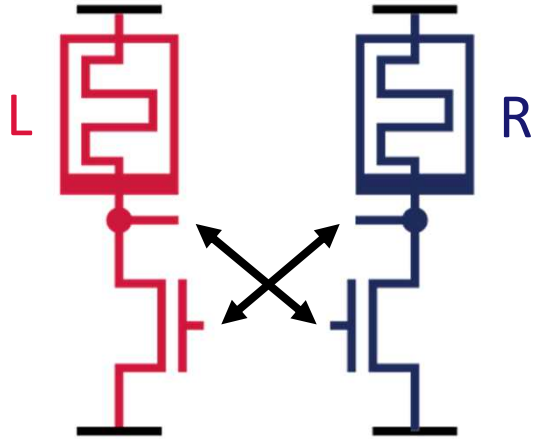
- 回路内部のエントロピーから応答を生成
  - 2回路相互の関係で値が決まる

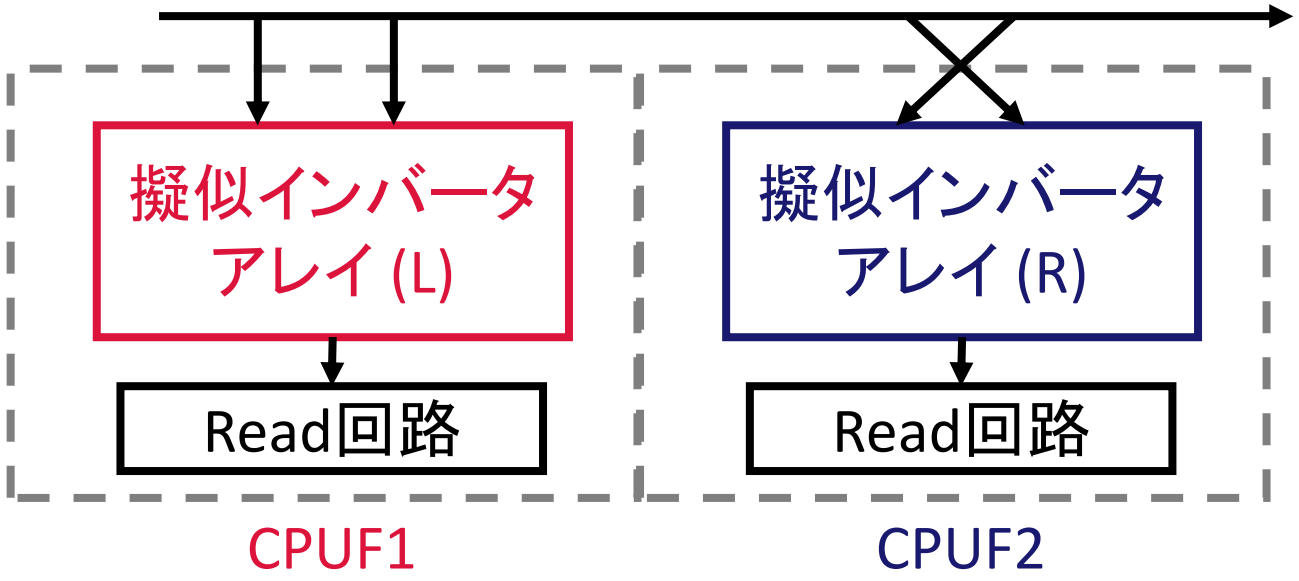


ダイシング時に書き込みが不可能となる

Coupled-INV CPUF：全体構成

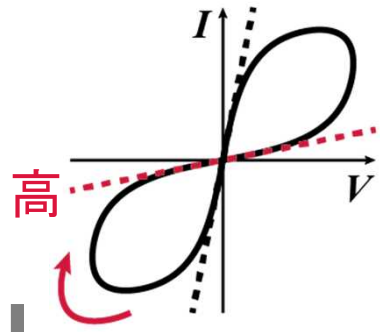
- CPUF回路
  - SRAM様の擬似インバータ対を分割してバラバラにもたせる
  - トランジスタおよびRRAMのばらつきにより値が決まる

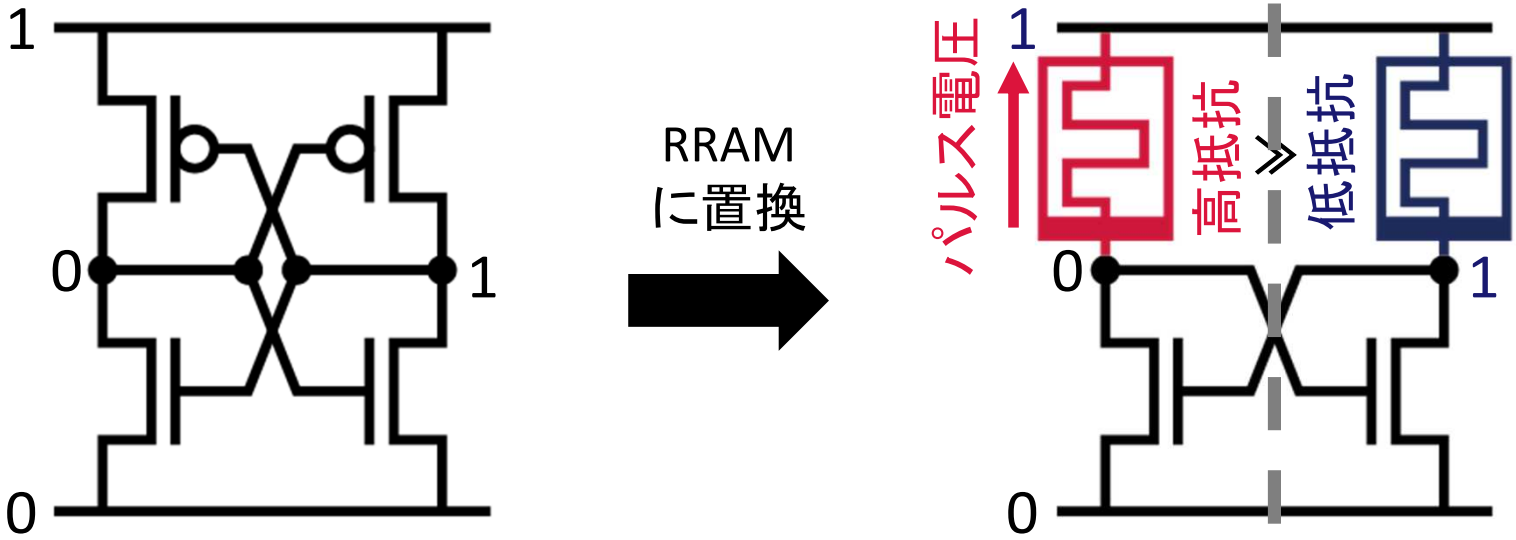




Coupled-INV CPUF：基本回路

- 疑似インバータを用いた疑似SRAM回路
- 安定状態：出力が(0, 1)あるいは(1, 0)
  - 低抵抗状態では1，高抵抗状態では0
  - 高抵抗状態のRRAMにのみ電圧がかかる

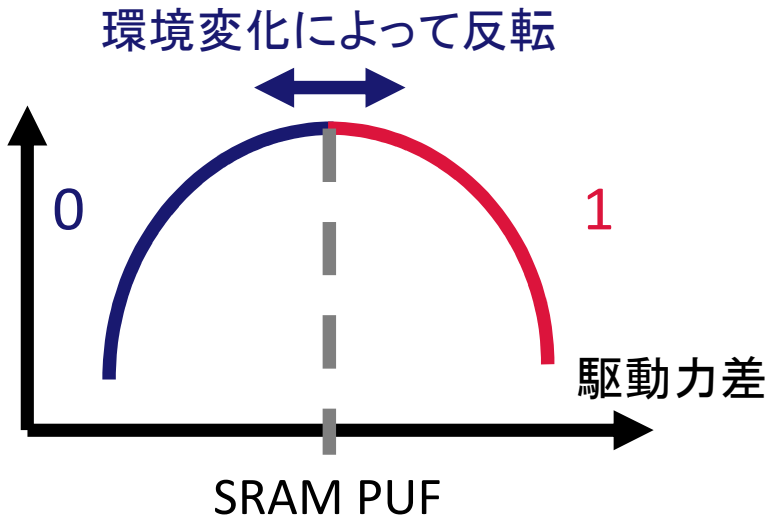


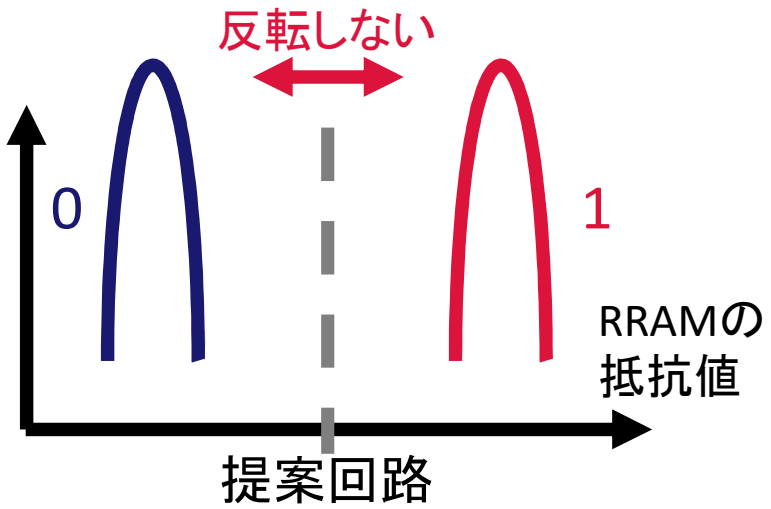


高抵抗RRAMをさらに高抵抗に

再現性の向上

- SRAM PUF等の再現性が低い課題
  - ばらつきが正規分布
- 提案回路はRRAMを用いてレスポンス生成
  - 双峰性の抵抗値分布





抵抗値の分布が0と1の境界に集中しない

シミュレーションによる評価

- 回路シミュレーション条件
  - 商用65nmプロセスを使用
  - Verilog-AベースのRRAMビヘイビアモデル[1]
  - トランジスタのしきい値電圧ばらつき: 正規分布
  - RRAMのギャップ初期値: 正規分布
- アレイ回路（最も大きいものを記載）
  - SRAM PUF : 16x16チップを100個
  - Shorted-INV CPUF: 16x16チップ 2 cloneを100個
  - Coupled-INV CPUF: 16x16チップ 2 cloneを100個
- 三つの評価指標について評価
  - CPUF: 等価性
  - PUF:予測不可能性，再現性

[1] P. Y. Chen et. al.

等価性 (equivalence)

- CPUFのレスポンスが互いに等価な割合
  - $e_{\mathrm{key},c}$: 全CPUFに同じチャレンジを与えるとき、一つでも不一致のresponseがあると0, 全一致で1
  - 等価性は、全チャレンジ、全チップ組合せに対する$e_{\mathrm{key},c}$の平均として定義

$$E = \frac{1}{|\mathcal{K}| \cdot |\mathcal{C}|} \sum_{\mathrm{key} \in \mathcal{K}} \sum_{c \in \mathcal{C}} e_{\mathrm{key},c}$$

	SRAM PUF	Shorted-INV	Coupled-INV
等価性E		1.000	1.000

すべてのCPUFで理想値1.0

予測不可能性

- Randomness (H)/Diffuseness (D)/Uniqueness (U)
  - チップ 全体/内/間 のばらつき
- CTW による圧縮率
  - レスポンスのエントロピー推定
- NIST 800-22による検定 (256ビットで評価)
  - 頻度/ブロック単位の頻度/累積和/連/ブロック単位の最長連

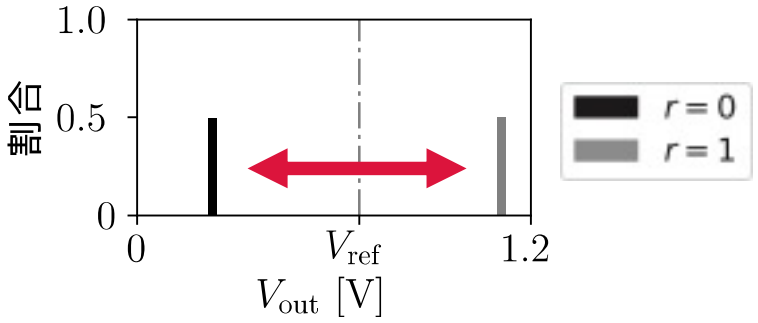
	SRAM PUF	Shorted-INV	Coupled-INV
H/D/U	0.99/1.00/0.99	0.99/1.00/0.99	0.99/1.00/0.99
CTW	1.016	1.017	1.016
NIST	PASS	PASS	PASS

いずれも十分予測不可能

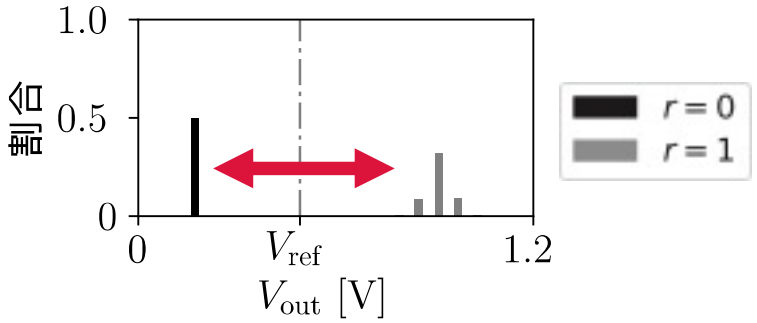
再現性

- 測定温度，電源電圧変化による応答の一致率
  - 測定温度変化（基準25℃）：-40℃から100℃
  - 電源電圧変化（基準1.2V）：-20%から+20%

	SRAM PUF	Shorted-INV CPUF	Coupled-INV CPUF
最低値	0.318	1.000	1.000



Shorted-INV CPUF



Coupled-INV CPUF

V_{out}の分布がV_{ref}近傍に集中しないため変動しない

企業への期待

- セキュリティ機能を有する不揮発メモリ・PUFの設計に関する共同研究を希望
  - 実デバイスによる試作
  - アプリケーション評価

- 模造品・互換品防止等のセキュリティ機能を必要とする企業には、本技術の導入が有効と考えられる

本技術に関する知的財産権

- 発明の名称：PUF回路群，PUF回路群の製造方法，PUF回路の使用方法，及びネットワークシステム
- 出願番号　：特願2018-154477
- 出願人　　：京都大学
- 発明者　　：佐藤高史、田中悠貴、辺松、廣本正之

新技術説明会
New Technology Presentation Meetings!

お問い合わせ先

国立大学法人京都大学内
関西ティー・エル・オー株式会社
京大事業部門　技術移転チーム
井下　陽平（いのした　ようへい）

TEL　　075-753-9150
FAX　　075-753-9169
e-mail　　inoshita@kansai-tlo.co.jp

thank you